实验目的和实验环境

实验目的

1、 掌握网络踩点的技巧

2、掌握网络扫描技巧

3、掌握常见的暴力破解方法

实验环境

1、kali-linux

需安装vm-tools

```
apt-get install open-vm-tools-desktop fuse
reboot
```

2、windows

任务1：网络踩点

选取一个熟悉的域名，尽可能的多获取该域名对于的信息如：

- 域名注册人以及联系方式
- 该域名对应的ip地址
- IP地址注册人以及联系方式
- IP地址所在的国家、城市

利用Google Hacking语法尽可能的获取该域名对应的网站的信息如：

- 后台登录系统网址
- 子域名
- 该网址用到的技术

参考文档：参考资料1-信息搜集-网络踩点.pdf

任务2：网络扫描

使用nmap或zenmap对ip地址148.70.46.9或靶机进行扫描，并得到如下结果

- 扫描靶机是否在线
- 扫描靶机开放了哪些tcp端口
- 扫描靶机开放了哪些udp端口
- 扫描靶机安装了什么操作系统
- 扫描靶机安装了哪些服务
- 输出扫描过程

ps：勿用综合扫描直接得到扫描结果，用多个nmap命令来获取上述结果

参考文档：参考资料2-信息搜集-网络扫描.pdf

任务3：暴力破解

子任务1：使用hydra 对ip地址为148.70.46.9的服务器进行SSH暴力破解获取登录密码

tips: 1、密码包含英文字母和数字 长度共9位

2、首位是大写英文字母

3、中间4位小写英文字母

4、后面四位数字

5、登录用户名root

ps：1、暴力破解成功的同学请勿将密码泄露给其他同学，将破解成功的密码告诉老师，并通知老师修改密码

2、破解成功后请勿破坏服务器的其他资料

3、第一个破解成功的同学，本次实验附加分额外增加50分，第二个破解成功的同学额外分依次递减5分

4、148.70.46.9破解不成功切换到owasp_broken靶机上练习

参考文档：参考资料3-暴利破解-Hydra.pdf

字典生成工具

子任务2：使用Burp Suite对网址http://148.70.46.9/login.html 进行暴力破解获取

tips: 1、密码包含英文字母和数字 长度共9位

2、前5位字母，与老师个人信息相关

4、后面四位数字

5、登录用户名wlaq

ps：1、暴力破解成功的同学请勿将密码泄露给其他同学，将破解成功的密码告诉老师，并通知老师修改密码

2、第一个破解成功的同学，本次实验附加分额外增加50分，第二个破解成功的同学额外分依次递减5分

参考文档：参考资料4-Burp Suite用法及暴力破解.pdf

实验要求

(1) 将实验过程截图，并保存，并在每个截图上标上自己的姓名和学号。

(2)将截图提交到腾讯课堂作业中